

13 MAG 2328

Approved: _____

Serrin Turner

Assistant United States Attorney

Before: HONORABLE FRANK MAAS
United States Magistrate Judge
Southern District of New York

UNITED STATES OF AMERICA

- v. -

ROSS WILLIAM ULBRICHT,
a/k/a "Dread Pirate Roberts,"
a/k/a "DPR,"
a/k/a "Silk Road,"

Defendant.

SEALED COMPLAINT

Violations of
21 U.S.C. § 846;
18 U.S.C. §§ 1030 & 1956

COUNTY OF OFFENSE:
NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

Christopher Tarbell, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE

(Narcotics Trafficking Conspiracy)

1. From in or about January 2011, up to and including in or about September 2013, in the Southern District of New York and elsewhere, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, intentionally and knowingly did combine, conspire, confederate, and agree together and with each other to violate the narcotics laws of the United States.

2. It was a part and an object of the conspiracy that ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, would and did distribute and possess with the intent to distribute controlled substances, in violation of Title 21, United States Code, Section 841(a)(1).

3. It was further a part and an object of the conspiracy that ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a

"DPR," a/k/a "Silk Road," the defendant, and others known and unknown, would and did deliver, distribute, and dispense controlled substances by means of the Internet, in a manner not authorized by law, and aid and abet such activity, in violation of Title 21, United States Code, Section 841(h).

4. The controlled substances involved in the offense included, among others, 1 kilogram and more of mixtures and substances containing a detectable amount of heroin, 5 kilograms and more of mixtures and substances containing a detectable amount of cocaine, 10 grams and more of mixtures and substances containing a detectable amount of lysergic acid diethylamide (LSD), and 500 grams and more of mixtures and substances containing a detectable amount of methamphetamine, its salts, isomers, and salts of its isomers, in violation of Title 21, United States Code, Sections 812, 841(a)(1), and 841(b)(1)(A).

Overt Acts

5. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. From in or about January 2011, up to and including in or about September 2013, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, owned and operated an underground website, known as "Silk Road," that provided a platform for drug dealers around the world to sell a wide variety of controlled substances via the Internet.

b. On or about March 29, 2013, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, in connection with operating the Silk Road website, solicited a Silk Road user to execute a murder-for-hire of another Silk Road user, who was threatening to release the identities of thousands of users of the site.

(Title 21, United States Code, Section 846.)

COUNT TWO

(Computer Hacking Conspiracy)

6. From in or about January 2011, up to and including in or about September 2013, in the Southern District of New York and elsewhere, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate

Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, intentionally and knowingly did combine, conspire, confederate, and agree together and with each other to commit computer hacking offenses in violation of Title 18, United States Code, Section 1030(a)(2).

7. It was a part and an object of the conspiracy that ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, would and did intentionally access computers without authorization, and thereby would and did obtain information from protected computers, for purposes of commercial advantage and private financial gain, and in furtherance of criminal and tortious acts in violation of the Constitution and the laws of the United States, in violation of Title 18, United States Code, Section 1030(a)(2).

Overt Acts

8. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. From in or about January 2011, up to and including in or about September 2013, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, owned and operated an underground website, known as "Silk Road," providing a platform facilitating the sale of illicit goods and services, including malicious software designed for computer hacking, such as password stealers, keyloggers, and remote access tools.

COUNT THREE

(Money Laundering Conspiracy)

9. From in or about January 2011, up to and including in or about September 2013, in the Southern District of New York and elsewhere, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, intentionally and knowingly did combine, conspire, confederate, and agree together and with each other to commit money laundering, in violation of Title 18, United States Code, Sections 1956(a)(1)(A)(i) and 1956(a)(1)(B)(i).

10. It was a part and an object of the conspiracy that ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, in offenses involving and affecting interstate and foreign commerce, knowing that the property involved in certain financial transactions represented proceeds of some form of unlawful activity, would and did conduct and attempt to conduct such financial transactions, which in fact involved the proceeds of specified unlawful activity, to wit, narcotics trafficking and computer hacking, in violation of Title 21, United States Code, Section 841, and Title 18, United States Code, Section 1030, respectively, with the intent to promote the carrying on of such specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i).

11. It was further a part and an object of the conspiracy that ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and others known and unknown, in offenses involving and affecting interstate and foreign commerce, knowing that the property involved in certain financial transactions represented proceeds of some form of unlawful activity, would and did conduct and attempt to conduct such financial transactions, which in fact involved the proceeds of specified unlawful activity, to wit, narcotics trafficking and computer hacking, in violation of Title 21, United States Code, Section 841, and Title 18, United States Code, Section 1030, respectively, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

Overt Acts

12. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. From in or about January 2011, up to and including in or about September 2013, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, owned and operated an underground website, known as "Silk Road," providing a platform facilitating the sale of controlled substances and malicious software, among other illicit goods and services, and further facilitating the laundering of proceeds from such sales, through the use of a

payment system based on Bitcoins, an anonymous form of digital currency.

b. At some point during the time period from January 2011 to September 2013, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, added a Bitcoin "tumbler" to the Silk Road payment system to further ensure that illegal transactions conducted on the site could not be traced to individual users.

(Title 18, United States Code, Section 1956(h).)

* * *

The bases for my knowledge and for the foregoing charges are, in part, as follows:

13. I have been a Special Agent with the FBI for approximately five years. I am currently assigned to a cybercrime squad within the FBI's New York Field Office. I have been personally involved in the investigation of this matter, along with agents of the Drug Enforcement Administration, the Internal Revenue Service, and Homeland Security Investigations. This affidavit is based upon my investigation, my conversations with other law enforcement agents, and my examination of reports, records, and other evidence. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

OVERVIEW

14. As detailed below, from in or about January 2011, up to and including in or about September 2013, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, has owned and operated an underground website known as "Silk Road." Throughout that time, the Silk Road website has served as a sprawling black-market bazaar, where illegal drugs and other illicit goods and services have been regularly bought and sold by the site's users.

15. In creating Silk Road, ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, deliberately set out to establish an online criminal

marketplace outside the reach of law enforcement or governmental regulation. ULBRICHT has sought to achieve this end by anonymizing activity on Silk Road in two ways. First, ULBRICHT has operated Silk Road on what is known as "The Onion Router" or "Tor" network ("Tor"), a special network on the Internet designed to make it practically impossible to physically locate the computers hosting or accessing websites on the network. Second, ULBRICHT has required all transactions on Silk Road to be paid with "Bitcoins," an electronic currency designed to be as anonymous as cash.

16. Based on my training and experience, Silk Road has emerged as the most sophisticated and extensive criminal marketplace on the Internet today. The site has sought to make conducting illegal transactions on the Internet as easy and frictionless as shopping online at mainstream e-commerce websites. The Government's investigation has revealed that, during its two-and-a-half years in operation, Silk Road has been used by several thousand drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services to well over a hundred thousand buyers, and to launder hundreds of millions of dollars deriving from these unlawful transactions. All told, the site has generated sales revenue totaling over 9.5 million Bitcoins and collected commissions from these sales totaling over 600,000 Bitcoins. Although the value of Bitcoins has varied significantly during the site's lifetime, these figures are roughly equivalent today to approximately \$1.2 billion in sales and approximately \$80 million in commissions.

17. ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, has controlled and overseen all aspects of Silk Road. ULBRICHT has maintained the computer infrastructure and programming code underlying the Silk Road website; he has determined vendor and customer policies, including deciding what can be sold on the site; he has managed a small staff of online administrators who have assisted with the day-to-day operation of the site; and he alone has controlled the massive profits generated from the operation of the business. ULBRICHT has assumed these roles fully aware of the illegal nature of his enterprise. He has sought throughout to ensure the anonymity of the drug dealers and other illegal vendors operating on Silk Road, as well as to conceal his own identity as the owner and operator of the site. Moreover, ULBRICHT has been willing to pursue violent means to maintain his control of the website and the illegal proceeds it generates for him.

BACKGROUND ON SILK ROAD

Design of the Silk Road Website and the Tor Network

18. In the course of this investigation, I have gained extensive familiarity with the Silk Road website through various means, including undercover activity on the website by myself and other law enforcement agents, as well as forensic analysis of computer servers used to operate the Silk Road website that have been located and imaged during the investigation. Based on my familiarity with the Silk Road website, I know the following about the site's design:

a. The Silk Road website provides a sales platform that allows vendors and buyers who are users of the site to conduct transactions online. The basic user interface resembles those of well-known online marketplaces.

b. However, unlike mainstream e-commerce websites, Silk Road is only accessible on the Tor network. Based on my training and experience, I know the following about Tor:

i. Tor is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true IP addresses of the computers on the network, and, thereby, the identities of the network's users.¹

ii. Although Tor has known legitimate uses, it also is known to be used by cybercriminals seeking to anonymize their online activity.

iii. Every communication sent through Tor is bounced through numerous relays within the network, and wrapped in numerous layers of encryption, such that it is practically impossible to trace the communication back to its true originating IP address.

iv. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites. Such "hidden services" operating on Tor have complex web addresses, generated by a

¹ Every computer device on the Internet has an Internet protocol or "IP" address assigned to it, which is used to route Internet traffic to or from the device. A device's IP address can be used to determine its physical location and, thereby, its user.

computer algorithm, ending in ".onion." For example, the address for the Silk Road website is currently "silkroadvb5piz3r.onion."

v. Websites with such ".onion" addresses can be accessed only using Tor browser software. However, such software can be easily downloaded for free on the Internet.

c. In order to access the Silk Road website, a user need only download Tor browser software onto his computer, and then type in Silk Road's ".onion" address into the user's Tor browser. Silk Road's ".onion" address can be found in various online forums and other websites on the ordinary Internet.

d. Upon being directed to the Silk Road website, a user is presented with a black screen containing a prompt for a username and password, as well as a link that says "click here to join." No further explanation about the site is given. Based on my training and experience, such cryptic login screens are often used by criminal websites in order to restrict access to users who already know about the illegal activity on the site (typically through word of mouth on Internet forums) and deliberately seek to enter.

e. Upon clicking the link on the Silk Road login screen to join the site, the user is prompted to create a username and password, and to identify the country where he is located. No other information is requested, and the country-location information entered by the user is not subject to any type of verification.

f. After entering a username and password, the user is then directed to Silk Road's homepage, a sample printout of which, printed on September 23, 2013, is attached hereto as Exhibit A.

g. At the top left corner of the homepage is a logo for the site, labeled "Silk Road anonymous market."

h. On the left side of the screen is a list titled "Shop by Category," which contains links to the various categories of items for sale on the site.

i. In the center of the screen is a collection of photographs reflecting a sample of the current listings on the site.

j. At the top of the screen is a link labeled "messages," which the user can click on to access Silk Road's "private message" system. This system allows users to send messages to one another through the site, similar to e-mails.

k. At the bottom right of the screen is a link labeled "community forums," which leads to an online forum where Silk Road users can post messages to "discussion threads" concerning various topics related to the site (the "Silk Road forum").

l. Also at the bottom right of the screen is a link labeled "wiki," which leads to a collection of "frequently asked questions" and other forms of guidance for site users (the "Silk Road wiki").

m. The bottom right of the screen also contains a third link labeled "customer service," which leads to a customer support page where users can "open a support ticket" and contact an "administrator," who, the page says, "will take care of you personally."

n. Clicking on any of the links to items for sale on the site brings up a webpage containing the details of the listing, including a description of the item, the price of the item, the username of the vendor selling it, and "reviews" of the vendor's "product" posted by previous customers. An example of such a listing is attached hereto as Exhibit B.

o. To buy an item listed, the user can simply click the link in the listing labeled "add to cart." The user is then prompted to supply a shipping address and to confirm the placement of the order.

p. Once the order is placed, it is processed through Silk Road's Bitcoin-based payment system, described further below.

Illegal Goods and Services Sold on the Silk Road Website

19. Based on my familiarity with the Silk Road website, I know the following about the illegal nature of the goods and services sold on the site:

a. The illegal nature of the items sold on Silk Road is readily apparent to any user browsing through its offerings. The vast majority of the goods for sale consist of illegal drugs of nearly every variety, which are openly advertised on the site

as such and are immediately and prominently visible on the site's home page.

b. As of September 23, 2013, there were nearly 13,000 listings for controlled substances on the website, listed under the categories "Cannabis," "Dissociatives," "Ecstasy," "Intoxicants," "Opioids," "Precursors," "Prescription," "Psychedelics," and "Stimulants," among others. Clicking on the link for a particular listing brings up a picture and description of the drugs being offered for sale, such as "HIGH QUALITY #4 HEROIN ALL ROCK" or "5gr UNCUT Crystal Cocaine!!"

c. The narcotics sold on the site tend to be sold in individual-use quantities, although some vendors sell in bulk. The offerings for sale on the site at any single time amount to multi-kilogram quantities of heroin, cocaine, and methamphetamine, as well as distribution quantities of other controlled substances, such as LSD.

d. In addition to illegal narcotics, other illicit goods and services are openly sold on Silk Road as well. For example, as of September 23, 2013:

i. There were 159 listings on the site under the category "Services." Most concerned computer-hacking services: for example, one listing was by a vendor offering to hack into Facebook, Twitter, and other social networking accounts of the customer's choosing, so that "You can Read, Write, Upload, Delete, View All Personal Info"; another listing offered tutorials on "22 different methods" for hacking ATM machines. Other listings offered services that were likewise criminal in nature. For example, one listing was for a "HUGE Blackmarket Contact List," described as a list of "connects" for "services" such as "Anonymous Bank Accounts," "Counterfeit Bills (CAD/GBP/EUR/USD)," "Firearms + Ammunition," "Stolen Info (CC [credit card], Paypal)," and "Hitmen (10+ countries)."

ii. There were 801 listings under the category "Digital goods," including offerings for pirated media content, hacked accounts at various online services such as Amazon and Netflix, and more malicious software. For example, one listing, titled "HUGE Hacking Pack **150+ HACKING TOOLS & PROGRAMS**," described the item being sold as a "hacking pack loaded with keyloggers, RATs, banking trojans, and other various malware."²

² A "keylogger" is a type of malicious software designed to monitor the keystrokes input into an infected computer and to transmit this data back to the hacker. A "RAT," or "remote

iii. There were 169 listings under the category "Forgeries," placed by vendors offering to produce fake driver's licenses, passports, Social Security cards, utility bills, credit card statements, car insurance records, and other forms of identity documents.

e. Not only are the goods and services offered on Silk Road overwhelmingly illegal on their face, but the illicit nature of the commerce conducted through the website is candidly recognized in the Silk Road wiki and the Silk Road forum. For example:

i. The Silk Road wiki contains a "Seller's Guide" and "Buyer's Guide" containing extensive guidance for users on how to conduct transactions on the site without being caught by law enforcement. The "Seller's Guide," for instance, instructs vendors to "vacuum seal" packages containing narcotics, in order to avoid detection by "canine or electronic sniffers." Meanwhile, the "Buyer's Guide" instructs buyers to "[u]se a different address" from the user's own address to receive shipment of any item ordered through the site, "such as a friend's house or P.O. box," from which the user can then "transport [the item] discreetly to its final destination."

ii. The Silk Road forum likewise contains extensive guidance on how to evade law enforcement, posted by users of the site themselves. For example, in a section of the forum labeled "Security - Tor, Bitcoin, cryptography, anonymity, security, etc.," there are numerous postings by users offering advice to other users on how they should configure their computers so as to avoid leaving any trace on their systems of their activity on Silk Road.

20. Since November of 2011, law enforcement agents participating in this investigation have made over 100 individual undercover purchases of controlled substances from Silk Road vendors, including purchases made from, and substances shipped to, the Southern District of New York. The substances purchased in these undercover transactions have been various Schedule I and II drugs, including ecstasy, cocaine, heroin, LSD, and others. Samples of these purchases have been laboratory-tested and have typically shown high purity levels of

access tool," is a type of malicious software designed to allow a hacker to remotely access and control an infected computer. A "banking Trojan" is a type of malicious software designed to steal an infected user's bank-account login credentials.

the drug the item was advertised to be on Silk Road. Based on the postal markings on the packages in which the drugs arrived, these purchases appear to have been filled by vendors located in over ten different countries, including the United States. Agents have also made undercover purchases of hacking services on Silk Road, including purchases of malicious software such as password stealers and remote access tools.

Silk Road's Bitcoin-Based Payment System

21. Based on my familiarity with the Silk Road website, I know the following concerning the payment system used to process purchases made through the site:

a. The only form of payment accepted on Silk Road is Bitcoins.

b. Based on my training and experience, I know the following about Bitcoins:

i. Bitcoins are an anonymous, decentralized form of electronic currency, existing entirely on the Internet and not in any physical form. The currency is not issued by any government, bank, or company, but rather is generated and controlled automatically through computer software operating on a "peer-to-peer" network. Bitcoin transactions are processed collectively by the computers composing the network.

ii. To acquire Bitcoins in the first instance, a user typically must purchase them from a Bitcoin "exchanger." In return for a commission, Bitcoin exchangers accept payments of currency in some conventional form (cash, wire transfer, etc.) and exchange the money for a corresponding number of Bitcoins, based on a fluctuating exchange rate. Exchangers also accept payments of Bitcoin and exchange the Bitcoins back for conventional currency, again, charging a commission for the service.

iii. Once a user acquires Bitcoins from an exchanger, the Bitcoins are kept in a "wallet" associated with a Bitcoin "address," designated by a complex string of letters and numbers. (The "address" is analogous to the account number for a bank account, while the "wallet" is analogous to a bank safe where the money in the account is physically stored.) Once a Bitcoin user funds his wallet, the user can then use Bitcoins in the wallet to conduct financial transactions, by transferring Bitcoins from his Bitcoin address to the Bitcoin address of another user, over the Internet.

iv. All Bitcoin transactions are recorded on a public ledger known as the "Blockchain," stored on the peer-to-peer network on which the Bitcoin system operates. The Blockchain serves to prevent a user from spending the same Bitcoins more than once. However, the Blockchain only reflects the movement of funds between anonymous Bitcoin addresses and therefore cannot by itself be used to determine the identities of the persons involved in the transactions. Only if one knows the identities associated with each Bitcoin address involved in a set of transactions is it possible to meaningfully trace funds through the system.

v. Bitcoins are not illegal in and of themselves and have known legitimate uses. However, Bitcoins are also known to be used by cybercriminals for money-laundering purposes, given the ease with which they can be used to move money anonymously.

c. Silk Road's payment system essentially consists of a Bitcoin "bank" internal to the site, where every user must hold an account in order to conduct transactions on the site.

d. Specifically, every user on Silk Road has a Silk Road Bitcoin address, or multiple addresses, associated with the user's Silk Road account. These addresses are stored on wallets maintained on servers controlled by Silk Road.

e. In order to make purchases on the site, the user must first obtain Bitcoins (typically from a Bitcoin exchanger) and send them to a Bitcoin address associated with the user's Silk Road account.

f. After thus funding his account, the user can then make purchases from Silk Road vendors. When the user purchases an item on Silk Road, the Bitcoins needed for the purchase are held in escrow (in a wallet maintained by Silk Road) pending completion of the transaction.

g. Once the transaction is complete, the user's Bitcoins are transferred to the Silk Road Bitcoin address of the vendor involved in the transaction. The vendor can then withdraw Bitcoins from the vendor's Silk Road Bitcoin address, by sending them to a different Bitcoin address, outside Silk Road, such as the address of a Bitcoin exchanger who can cash out the Bitcoins for real currency.

h. Silk Road charges a commission for every transaction conducted by its users. The commission rate varies, generally between 8 to 15 percent, depending on the size of the sale, i.e., the larger the sale, the lower the commission.

i. Silk Road uses a so-called "tumbler" to process Bitcoin transactions in a manner designed to frustrate the tracking of individual transactions through the Blockchain. According to the Silk Road wiki, Silk Road's tumbler "sends all payments through a complex, semi-random series of dummy transactions, . . . making it nearly impossible to link your payment with any coins leaving the site." In other words, if a buyer makes a payment on Silk Road, the tumbler obscures any link between the buyer's Bitcoin address and the vendor's Bitcoin address where the Bitcoins end up - making it fruitless to use the Blockchain to follow the money trail involved in the transaction, even if the buyer's and vendor's Bitcoin addresses are both known. Based on my training and experience, the only function served by such "tumblers" is to assist with the laundering of criminal proceeds.

Volume of Business Activity
Reflected on Silk Road Servers

22. During the course of this investigation, the FBI has located a number of computer servers, both in the United States and in multiple foreign countries, associated with the operation of Silk Road. In particular, the FBI has located in a certain foreign country the server used to host Silk Road's website (the "Silk Road Web Server"). Pursuant to a Mutual Legal Assistance Treaty request, an image of the Silk Road Web Server was made on or about July 23, 2013, and produced thereafter to the FBI. From personally participating in the forensic analysis of the image of the Silk Road Web Server, I have confirmed that Silk Road hosts a large volume of user activity and processes a huge number of financial transactions on a daily basis. For example:

a. As of July 23, 2013, there were approximately 957,079 registered user accounts reflected on the server.³ This does not necessarily equal the number of actual users of the

³ According to the country-location information provided by these users upon registering, 30 percent represented they were from the United States, 27 percent chose to be "undeclared," and the remainder claimed to hail from countries across the globe, including, in descending order of prevalence, the United Kingdom, Australia, Germany, Canada, Sweden, France, Russia, Italy, and the Netherlands.

website, since nothing prevents a user from creating multiple accounts. However, based on my training and experience, this volume of user accounts indicates that the site has been visited by hundreds of thousands of unique users.

b. During the 60-day period from May 24, 2013 to July 23, 2013, there were approximately 1,217,218 communications sent between Silk Road users through Silk Road's private-message system. Based on my training and experience, this volume of private messages reflects a large and highly active user base.

c. From February 6, 2011 to July 23, 2013, there were approximately 1,229,465 transactions completed on the site, involving 146,946 unique buyer accounts, and 3,877 unique vendor accounts. The total revenue generated from these sales was 9,519,664 Bitcoins, and the total commissions collected by Silk Road from the sales amounted to 614,305 Bitcoins. These figures are equivalent to roughly \$1.2 billion in revenue and \$79.8 million in commissions, at current Bitcoin exchange rates, although the value of Bitcoins has fluctuated greatly during the time period at issue.

d. The computer code used to run the Silk Road website reflects the use of certain Bitcoin wallets in the operation of Silk Road's escrow system. The balances in these wallets (obtained from another Silk Road-associated server located in the investigation) show hundreds of thousands of dollars passing in and out of the escrow system on a regular basis, as in the following sample of balances associated with the wallets taken over a two-day time period:

<u>Date/Time</u>	<u>Total Bitcoins</u>	<u>Approx. USD</u>
9/14/2013 6:00 UTC	18205.50649	\$2,548,770.91
9/14/2013 12:00 UTC	17420.92877	\$2,438,930.03
9/14/2013 18:00 UTC	17088.67959	\$2,358,237.79
9/15/2013 0:00 UTC	13950.06159	\$1,911,158.44
9/15/2013 6:00 UTC	16143.52567	\$2,195,519.49
9/15/2013 12:00 UTC	15955.46307	\$2,217,809.37
9/15/2013 18:00 UTC	16069.43546	\$2,233,651.53

Based on my training and experience, this flow of funds reflects a brisk business being conducted within Silk Road's illegal marketplace, with users regularly adding funds to their accounts and vendors regularly cashing out.

BACKGROUND ON "DREAD PIRATE ROBERTS,"
OWNER AND OPERATOR OF SILK ROAD

23. Based on my knowledge of the Silk Road website, I am familiar with an administrator of the site who goes by the username "Dread Pirate Roberts," commonly referred to by Silk Road users as "DPR" (hereafter, "DPR"). Based on my review of DPR's communications on the Silk Road website, as described more fully below, it is clear that DPR is the owner and operator of Silk Road and has been ultimately responsible for running the criminal enterprise it represents. DPR has controlled every aspect of Silk Road's operation, including: the server infrastructure and programming code underlying its website; the user policies governing, among other things, what can be sold on the site; the administrative staff responsible for customer support and other day-to-day functions; and the profits generated as commissions from vendor sales. Moreover, DPR's communications reveal that he has taken it upon himself to police threats to the site from scammers and extortionists, and has demonstrated a willingness to use violence in doing so.

Control of Server Infrastructure

24. Based on my familiarity with the Silk Road forum, I know that DPR has an account on the forum, and that his postings from the account reflect his control of the servers and computer code used to run the Silk Road website. Specifically, from reviewing DPR's postings to the forum from this account, I know the following:

a. The Silk Road forum, in its current form, was created on or about June 18, 2011. DPR's first posting to the forum was made the same day. At that time, DPR's username on the forum was simply "Silk Road." His June 18 posting apologized for a recent service outage, explaining that the forum had been changed and that now "[w]e have it running on a separate server." The message thanked users for their patience and was signed "Silk Road Staff."

b. DPR continued posting messages to the forum under the username "Silk Road" until early February 2012, when he changed his name to "Dread Pirate Roberts." Specifically, in or about early February, 2012, DPR posted the following message from his forum account, still associated with the username "Silk Road" at the time:

Who is Silk Road? Some call me SR, SR admin or just Silk Road. But isn't that confusing? I am Silk Road,

the market, the person, the enterprise, everything.
But Silk Road has matured and I need an identity
separate from the site and the enterprise of which I
am now only a part. I need a name.

On February 5, 2012, DPR announced, from this same account, "drum roll please..... my new name is: Dread Pirate Roberts." Thereafter, the username associated with the account changed from "Silk Road" to "Dread Pirate Roberts." The moniker is an apparent reference to a fictional character from the movie "The Princess Bride."

c. Throughout the period from June 18, 2011 to the present, DPR's postings from his Silk Road forum account, under both the username "Silk Road" and the username "Dread Pirate Roberts," make clear that he has controlled the technical infrastructure underlying Silk Road's operation. Among other things, DPR has regularly used the forum to post information concerning service problems with the Silk Road website and his efforts to resolve such problems. For example:

i. On or about February 13, 2012, DPR posted a message on the forum in response to problems users were having withdrawing Bitcoins from their Silk Road accounts. DPR acknowledged the problem and explained what was being done to fix it: "[W]e are still having problems. I am going to roll back the withdrawal system to a configuration known to work and re-evaluate the whole thing. . . . I'll keep this thread updated with progress." In an update posted the next morning, DPR stated: "We are looking at up to 24 more hours until withdrawals can start flowing again. . . . Really sorry, but I think we'll be good to go after this." Later in the day, DPR provided a further update: "Withdrawals are now flowing again. Thank you everyone for your patience throughout this process." Based on my training and experience, these postings and others like them, announcing service changes to the Silk Road website prior to their implementation, show that DPR has been responsible for these changes and has controlled the server infrastructure necessary to make them.

ii. On or about December 1, 2011, DPR announced that he had changed the .onion address for the Silk Road website, stating: "Silk Road now resides at a new, more easily remembered url [i.e., URL address]. Please update your bookmarks and memorize it: silkroadvb5piz3r.onion." One user responded to the posting to suggest that DPR "leave the old addy [address] pointing at the site for a week or two as well so folks get used to it." DPR responded, "I wanted to do that, but

it conflicts with the site code :(" Based on my training and experience, this posting reflects that DPR himself has been responsible for programming the computer code underlying the Silk Road website.

iii. On or about October 19, 2011, DPR posted a message concerning an outage of the Silk Road website, explaining: "We are having to rebuild the site from a backup." DPR assured the site's users: "There was no security breach or anything to worry about that lead [sic] to this situation. We lease server space in different locations around the globe through unaware 3rd parties. We do this to hide the identities of those that run Silk Road in the event of a security breach in one of the servers. Unfortunately this means we have to deal with some unreliable people" In an update posted two days later, on October 21, 2011, DPR stated: "The light at the end of the tunnel is getting bigger! We have a full capacity server online and are in the process of configuring it." The next day, October 22, 2011, DPR posted another update, stating: "The site just went live. The new server is more powerful and secure than the one we were on before the outage and is leased through a much more professional proxy, so I have high hopes that it will last us a long time." Based on my training and experience, these postings evidence that DPR has been responsible for leasing and maintaining the computer servers used to operate the Silk Road website. Moreover, based on my training and experience, DPR's references to leasing servers through third-party "proxies" in order to "hide the identities of those that run Silk Road" reflect his awareness of the illegal nature of the Silk Road enterprise.

Control of Site Policy

25. DPR has used the Silk Road forum to announce not only technical updates to the Silk Road website, but also changes to Silk Road customer policies - evidencing that he has been the one who sets those policies. For example:

a. On January 9, 2012, DPR posted a message titled, "State of the Road Address," in which he announced, among other things, a change to Silk Road's commission rate: whereas Silk Road had previously charged a "flat commission rate," DPR explained that the site now planned to "charge a higher amount for low priced items and a lower amount for high priced items." The next day, after many users complained about the change, DPR posted a reply, stating: "Whether you like it or not, I am the captain of this ship. You are here voluntarily and if you don't

like the rules of the game, or you don't trust your captain, you can get off the boat."

b. On August 5, 2011, DPR posted a message titled, "forgeries," stating: "We are happy to announce a new category in the marketplace called Forgeries. In this category, you will find offers for forged, government issued documents including fake ids and passports. This category comes with some restrictions, however. Sellers may not list forgeries of any privately issued documents such as diplomas/certifications, tickets or receipts. Also, listings for counterfeit currency are still not allowed in the money section." This posting evidences that DPR has controlled the types of goods and services allowed to be sold on Silk Road, and that he knowingly has permitted the sale of illegal items, such as fraudulent identity documents, on the site.

c. On February 27, 2012, DPR posted a message announcing "a new feature called Stealth Mode," targeted at the site's "superstar vendor[s]" who consider themselves at particular "risk of becoming a target for law enforcement." The posting explained that the listings of a vendor operating in "stealth mode" would not be visible to users searching or browsing the site. Instead, only users who already knew the specific address of the vendor's page on Silk Road would be able to access the vendor's listings, by traveling to the vendor's page directly. This posting again evidences not only that DPR has been aware that the vendors on Silk Road are engaged in illicit trade, but also that he has specifically designed the site to facilitate such trade.

Management of Administrative Staff

26. The communications recovered from the Silk Road Web Server also show that DPR manages a small staff of administrators who assist with the day-to-day operation of the site. Based on my familiarity with these administrators' forum postings and private messages, I know that they have been responsible for monitoring user activity on Silk Road for problems, responding to customer service inquiries, and resolving disputes between buyers and vendors. Moreover, forensic analysis of the Silk Road Web Server confirms that these administrators have special permission settings associated with their Silk Road accounts, allowing them to take various administrative actions on the Silk Road marketplace, such as closing user accounts, removing user postings, reversing transactions, or resetting passwords.

27. From reviewing DPR's private-message communications with these administrators, I know that DPR has functioned as their supervisor and that the administrators have reported to and taken instructions from DPR on a regular basis. For example, the communications show the administrators regularly asking DPR for guidance on how to respond to particular user inquiries or how to handle particular problems that have arisen on the site. The communications also include "weekly reports" sent to DPR by the administrators, summarizing actions they have taken with respect to particular vendors and customers over the course of the week, and listing any important issues requiring DPR's attention. DPR's communications also reflect the administrators routinely checking in with him concerning their work schedule, asking him in advance for permission to take leave, and otherwise addressing him as employees would an employer. One of the administrators, for example, has specifically referred to DPR as "boss" and "captain" in communicating with him.

28. Further, I have reviewed the account pages of these administrators, recovered from the Silk Road Web Server, which reflect the history of their Bitcoin transactions on the site. Their transaction histories reflect that they have received regular weekly payments of Bitcoins, equivalent to \$1,000 to \$2,000 per week, on average. The payments have been sent to them from a Silk Road account labeled "admin," indicating that the payments have been compensation for their services as administrators. Moreover, from reviewing the administrators' private messages, I know that, after receiving such payments, the administrators sometimes have sent messages to DPR thanking him for the money.

Control over Silk Road Sales Proceeds

29. The contents of the Silk Road Web Server include DPR's own user account page, which reflects, among other things, his history of Bitcoin transactions on the site. DPR's transaction history indicates that he receives a continuous flow of Bitcoins into his Silk Road account. For example, on July 21, 2013 alone, DPR received approximately 3,237 separate transfers of Bitcoins into his account, totaling approximately \$19,459. Virtually all of these transactions are labeled "commission" in the "notes" appearing next to them, indicating that the money represents commissions from Silk Road sales. DPR's account page further displays the total amount of Bitcoins deposited in his Silk Road account, which, as of July 23, 2013, equaled more than \$3.4 million. Based on analysis of the Silk Road Web Server,

this was, by far, the largest account balance held by any Silk Road user at the time.

DPR's Willingness to Use Violence
to Protect His Interests in Silk Road

30. DPR's private communications recovered from the Silk Road Web Server further reveal that DPR has acted as a law unto himself in deciding how to deal with problems affecting Silk Road, and that he has been willing to pursue violent means when he deems that the problem calls for it.

31. For example, DPR's private-message communications from March and April 2013 reveal at least one occasion when DPR solicited a murder-for-hire of a certain Silk Road user, who was attempting to extort money from DPR at the time, based on a threat to release the identities of thousands of Silk Road users. Specifically, the messages reveal the following:

a. Beginning on March 13, 2013, a Silk Road vendor known as "FriendlyChemist" began sending threats to DPR through Silk Road's private message system. In these messages, FriendlyChemist stated that he had a long list of real names and addresses of Silk Road vendors and customers that he had obtained from hacking into the computer of another, larger Silk Road vendor. FriendlyChemist threatened to publish the information on the Internet unless DPR gave him \$500,000, which FriendlyChemist indicated he needed to pay off his narcotics suppliers.

b. In one message to DPR dated March 14, 2013, FriendlyChemist elaborated on the consequences for Silk Road if he followed through on this threat:

what do u . . . think will happen if thousands of usernames, ordr amounts, addresses get leaked? all those people will leave sr [Silk Road] and be scared to use it again. those vendors will all be busted and all there customers will be exposed too and never go back to sr.

c. On March 15, 2013, FriendlyChemist provided DPR a sample of the usernames, addresses, and order information he intended to leak. Also, as proof that he had obtained the data from the vendor whose computer he claimed to have hacked, FriendlyChemist supplied the vendor's username and password on Silk Road so that DPR could verify it.

d. On March 20, 2013, DPR wrote to FriendlyChemist, stating: "Have your suppliers contact me here so I can work something out with them."

e. On March 25, 2013, a Silk Road user named "redandwhite" contacted DPR, stating: "I was asked to contact you. We are the people friendlychemist owes money to. . . . What did you want to talk to us about?"

f. On March 26, 2013, DPR wrote to redandwhite, stating, "Just to be clear, I do not owe him any money. . . . I'm not entirely sure what the best action to take is, but I wanted to be in communication with you to see if we can come to a conclusion that works for everyone. FriendlyChemist aside, we should talk about how we can do business. Obviously you have access to illicit substances in quantity, and are having issues with bad distributors. If you don't already sell here on Silk Road, I'd like you to consider becoming a vendor."

g. Later on March 26, 2013, redandwhite responded: "If you can get FriendlyChemist to meet up with us, or pay us his debt then I'm sure I would be able to get people in our group to give this online side of the business a try."

h. On March 27, 2013, DPR wrote back: "In my eyes, FriendlyChemist is a liability and I wouldn't mind if he was executed I'm not sure how much you already know about the guy, but I have the following info and am waiting on getting his address." DPR provided a name for FriendlyChemist and stated that he lived in White Rock, British Columbia, Canada, with "Wife + 3 kids." DPR added: "Let me know if it would be helpful to have his full address."

i. Meanwhile, after not hearing anything back from DPR since March 20, 2013, FriendlyChemist sent a message to DPR on March 29, 2013, stating: "u leave me no choice i want 500k usd withn 72hrs or i am going to post all the info i have. . . . i hate to do this but i need the money or im going to release it all. over 5000 user details and about 2 dozen vender identities. wats it going to be?"

j. Several hours later on March 29, 2013, DPR sent a message to "redandwhite," stating that "FriendlyChemist" is "causing me problems," and adding: "I would like to put a bounty on his head if it's not too much trouble for you. What would be an adequate amount to motivate you to find him? Necessities

like this do happen from time to time for a person in my position."

k. After redandwhite asked DPR what sort of problem FriendlyChemist was causing him, DPR responded, in a message dated March 30, 2013: "[H]e is threatening to expose the identities of thousands of my clients that he was able to acquire [T]his kind of behavior is unforgivable to me. Especially here on Silk Road, anonymity is sacrosanct." As to the murder-for-hire job he was soliciting, DPR commented that "[i]t doesn't have to be clean."

l. Later that same day, redandwhite sent DPR a message quoting him a price of \$150,000 to \$300,000 "depending on how you want it done" - "clean" or "non-clean."

m. On March 31, 2013, DPR responded: "Don't want to be a pain here, but the price seems high. Not long ago, I had a clean hit done for \$80k. Are the prices you quoted the best you can do? I would like this done asap as he is talking about releasing the info on Monday."

n. Through further messages exchanged on March 31, 2013, DPR and redandwhite agreed upon a price of 1,670 Bitcoins - approximately \$150,000 - for the job. In DPR's message confirming the deal, DPR included a transaction record reflecting the transfer of 1,670 Bitcoins to a certain Bitcoin address.

o. Several hours later on March 31, 2013, redandwhite wrote back: "I received the payment. . . . We know where he is. He'll be grabbed tonight. I'll update you."

p. Approximately 24 hours later, redandwhite updated DPR, stating: "Your problem has been taken care of. . . . Rest easy though, because he won't be blackmailing anyone again. Ever."

q. Subsequent messages reflect that, at DPR's request, redandwhite sent DPR a picture of the victim after the job was done, with random numbers written on a piece of paper next to the victim that DPR had supplied. On April 5, 2013, DPR wrote redandwhite: "I've received the picture and deleted it. Thank you again for your swift action."

32. Although I believe the foregoing exchange demonstrates DPR's intention to solicit a murder-for-hire, I have spoken with

Canadian law enforcement authorities, who have no record of there being any Canadian resident with the name DPR passed to redandwhite as the target of the solicited murder-for-hire. Nor do they have any record of a homicide occurring in White Rock, British Columbia on or about March 31, 2013.

Identification of "Dread Pirate Roberts"
as ROSS WILLIAM ULBRICHT, the Defendant

33. As described in detail below, DPR has been identified through this investigation as ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant. According to ULBRICHT's profile on "linkedin.com" ("LinkedIn"), a professional networking website where members can post information about their work backgrounds and interests, ULBRICHT, 29 years old, graduated from the University of Texas with a Bachelor of Science degree in Physics in 2006. From 2006 to 2010, he attended graduate school at the University of Pennsylvania School of Materials Science and Engineering. However, ULBRICHT states in his LinkedIn profile that, after this time in graduate school, his "goals" subsequently "shifted." ULBRICHT elaborates, obliquely, that he has since focused on "creating an economic simulation" designed to "give people a first-hand experience of what it would be like to live in a world without the systemic use of force" by "institutions and governments." Based on the evidence below, I believe that this "economic simulation" referred to by ULBRICHT is Silk Road.

34. First, I have spoken with another agent involved in this investigation ("Agent-1"), who has conducted an extensive search of the Internet in an attempt to determine how and when the Silk Road website was initially publicized among Internet users. The earliest such publicity found by Agent-1 is a posting dated January 27, 2011, on an online forum hosted at www.shroomery.org, an informational website catering to users of "magic mushrooms" ("Shroomery"). The posting, titled "anonymous market online?," was made by a user identified only by his username, "altoid." The posting stated as follows:

I came across this website called Silk Road. It's a Tor hidden service that claims to allow you to buy and sell anything online anonymously. I'm thinking of buying off it, but wanted to see if anyone here had heard of it and could recommend it. I found it through silkroad420.wordpress.com, which, if you have a tor browser, directs you to the real site at <http://tydgccykixpbu6uz.onion>. Let me know what you think...

This was the only message ever posted on the Shroomery forum by "altoid," indicating, based on my training and experience, that he had joined the forum solely to post this message.

35. In the Shroomery posting, "altoid" stated that he "found out" about Silk Road through "silkroad420.wordpress.com," where he stated that Tor users could be redirected to Silk Road on Tor. The address "silkroad420.wordpress.com" is an account on a blogging site known as "Wordpress." According to records obtained from Wordpress, the "silkroad420" account was created on January 23, 2011 - only four days before the posting by "altoid" on the Shroomery blog. (The account was created anonymously by someone who, based on the IP address they used, was using a Tor connection to access the Internet.)

36. After the Shroomery posting made on January 27, 2011, the next reference to Silk Road on the Internet found by Agent-1 is a posting made two days later, on January 29, 2011, at "bitcointalk.org," an online discussion forum relating to Bitcoins ("Bitcoin Talk"). This posting, too, was made by someone using the username "altoid." The posting appeared in a long-running discussion thread started by other Bitcoin Talk users, concerning the possibility of operating a Bitcoin-based "heroin store." In his posting, "altoid" stated:

What an awesome thread! You guys have a ton of great ideas. Has anyone seen Silk Road yet? It's kind of like an anonymous amazon.com. I don't think they have heroin on there, but they are selling other stuff. They basically use bitcoin and tor to broker anonymous transactions. It's at <http://tydgccykixpbu6uz.onion>. Those not familiar with Tor can go to silkroad420.wordpress.com for instructions on how to access the .onion site.

Let me know what you guys think

37. Based on my training and experience, the two postings created by "altoid" on Shroomery and Bitcoin Talk appear to be attempts to generate interest in the site. The fact that "altoid" posted similar messages about the site on two very different discussion forums, two days apart, indicates that "altoid" was visiting various discussion forums around this time where Silk Road might be of interest and seeking to publicize the site among the forum users - which, based on my training and experience, is a common online marketing tactic for new

websites. Moreover, the fact that "altoid" ended both messages with "Let me know what you guys think" indicates that "altoid" was not merely interested in sharing his own experience with Silk Road but wanted to collect feedback from other users, again, consistent with an effort to market and improve the site.

38. From further reviewing the Bitcoin Talk forum, Agent-1 located another posting on the forum by "altoid," made on October 11, 2011, approximately eight months after his posting about Silk Road. In this later posting, made in a separate and unrelated discussion thread, "altoid" stated that he was looking for an "IT pro in the Bitcoin community" to hire in connection with "a venture backed Bitcoin startup company." The posting directed interested users to send their responses to "rossulbricht at gmail dot com" - indicating that "altoid" uses the e-mail address "rossulbricht@gmail.com" (the "Ulbricht Gmail Account").

39. According to subscriber records obtained from Google, the Ulbricht Gmail Account is registered to a "Ross Ulbricht." The records indicate that Ulbricht has an account at Google+, a Google-based social networking service. From visiting Ulbricht's publicly accessible profile on Google+, I know that Ulbricht's Google+ profile includes a picture of him, which matches a picture of the LinkedIn profile for "Ross Ulbricht" referenced above in paragraph 33.

40. From visiting Ulbricht's Google+ page, I also know that it contains links to a specific website that DPR has regularly cited in his forum postings. Specifically:

a. Ulbricht's Google+ profile includes a list of Ulbricht's favorite YouTube videos, which includes a number of videos originating from "mises.org," the website of an entity dubbed the "Mises Institute." According to its website, the "Mises Institute" considers itself the "world center of the Austrian School of economics." The website allows visitors to sign up for user accounts on the site and to create a user profile. Through visiting a publicly accessible archived version of the site, I have found a user profile for a "Ross Ulbricht" on the site, which contains a picture of the user that matches the picture of "Ross Ulbricht" appearing on his Google+ profile and LinkedIn profile.

b. Based on my familiarity with DPR's postings on the Silk Road forum, I know that DPR's user "signature" in the forum includes a link to the "Mises Institute" website (one of only two links included in his signature). Moreover, in certain

forum postings, DPR has cited the "Austrian Economic theory" and the works of Ludwig von Mises and Murray Rothbard - economists closely associated with the "Mises Institute" - as providing the philosophical underpinnings for Silk Road.

41. The investigation has also uncovered evidence that, in early June 2013, Ulbricht was residing in San Francisco, California, near an Internet café from which someone logged into a server used to administer the Silk Road website on June 3, 2013. Specifically:

a. I have reviewed records obtained from Google containing logs of the IP addresses used to log into the Ulbricht Gmail Account from January 13, 2013 to June 20, 2013. The IP logs show the account being regularly accessed throughout this time period from a certain Comcast IP address. According to records obtained from Comcast, this IP address was assigned at the time of these logins to a certain address located on Hickory Street in San Francisco, California. The address is associated with another individual whom I know to be a friend of Ulbricht in San Francisco (the "Friend"), whom Ulbricht went to live with when he moved to San Francisco in or about September 2012, according to a video posted on YouTube in which they both appear and make statements to that effect.

b. Based on my review of DPR's private-message communications recovered from the Silk Road Web Server, I know that DPR has regularly specified the Pacific time zone when referring to the time. For example, in one private message, dated April 18, 2013, DPR told another Silk Road user, "It's nearly 4pm PST. I need to run some errands." Based on my training and experience, I believe this tendency indicates that DPR is located in the Pacific time zone - which, of course, is the time zone for San Francisco, California.

c. Further, based on forensic analysis of the Silk Road Web Server, I know that the server includes computer code that was once used to restrict administrative access to the server, so that only a user logging into the server from a particular IP address, specified in the code, could access it. Based on my training and experience, and my familiarity with how server access is commonly configured, I believe this IP address was for a virtual private network server ("VPN Server") - essentially a secure gateway through which DPR could remotely login to the Silk Road Web Server from his own computer. The IP address for the VPN Server resolves to a server hosted by a certain server-hosting company, from which I have subpoenaed

records concerning the VPN Server. The records show that the contents of the VPN Server were erased by the customer leasing it.⁴ However, the records reflect the IP address the customer used to access the VPN Server during the last login to the server, which was on June 3, 2013. This IP address is a Comcast address that, according to records subpoenaed from Comcast, resolves to an Internet café on Laguna Street in San Francisco, California. This café is located less than 500 feet away from the Friend's address on Hickory Street regularly used by Ulbricht to log in to the Ulbricht Gmail Account - including at various times on June 3, 2013, according to Google records.

d. Based on my training and experience, this evidence places the administrator of Silk Road, that is, DPR, in the same approximate geographic location, on the same day, as Ulbricht.

42. The investigation has also uncovered evidence that, by July 2013, Ulbricht had moved to a different San Francisco address, where he was shipped a package containing multiple counterfeit identification documents, at the same time that DPR is known to have been seeking such documents on Silk Road. Specifically:

a. From reviewing an investigative report obtained from U.S. Customs and Border Protection ("CBP"), I have learned the following:

i. On or about July 10, 2013, CBP intercepted a package from the mail inbound from Canada as part of a routine border search. The package was found to contain nine counterfeit identity documents. Each of the counterfeit identification documents was in a different name yet all

⁴ The code containing the IP address for the VPN Server is "commented out" on the Silk Road Web Server, meaning that it was no longer active as of July 23, 2013, when the image of the server was made. From reviewing DPR's private-message communications recovered from the Silk Road Web Server, I know that, on May 24, 2013, a Silk Road user sent him a private message warning him that "some sort of external IP address" was "leaking" from the site, and listed the IP address of the VPN Server. Based on my training and experience, I believe that in light of this warning DPR deactivated the code containing the VPN Server IP Address, deleted the contents of the VPN Server, and changed the way he accessed the Silk Road Web Server thereafter.

contained a photograph of the same person. The package was directed to an address located on 15th Street in San Francisco, California (the "15th Street Address").

ii. On or about July 26, 2013, agents from Homeland Security Investigations ("HSI") visited the 15th Street Address to investigate further. Agents found a residence there, where they encountered ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, who matched the photographs on the counterfeit identification documents in the package.

iii. The agents showed ULBRICHT a photo of one of the seized counterfeit identity documents, which was a California driver's license bearing ULBRICHT's photo and true date of birth, but bearing a name other than his. ULBRICHT generally refused to answer any questions pertaining to the purchase of this or other counterfeit identity documents. However, ULBRICHT volunteered that "hypothetically" anyone could go onto a website named "Silk Road" on "Tor" and purchase any drugs or fake identity documents the person wanted.

iv. ULBRICHT provided the agents with his true government-issued Texas driver's license. He explained that he sublet a room at the 15th Street Address for \$1,000 in monthly rent, which he paid in cash. ULBRICHT stated that there were two other housemates currently residing with him in the house, both of whom knew him by the fake name "Josh."

v. The agents also spoke with one of ULBRICHT's housemates at the address, who stated that ULBRICHT, whom he knew as "Josh," was always home in his room on the computer.

b. Based on my review of DPR's private messages recovered from the Silk Road Web Server, I know that, in June and July 2013, DPR had several communications with other Silk Road users in which he expressed interest in acquiring fake identity documents. For example:

i. In one exchange of messages, dated July 8, 2013, DPR told another Silk Road user that he "needed a fake ID" that he intended to use to "rent servers," explaining that he was "building up my stock of servers." Based on my training and experience, I know that server-hosting companies often require customers to provide some form of identity documents in order to validate who they are. Accordingly, I believe that DPR was seeking fake identity documents that he could use to rent servers under false identities.

ii. In another exchange of messages, dated June 1, 2013, DPR and another Silk Road user - "redandwhite," the same user with whom DPR solicited the murder-for-hire described above - agreed to communicate at a certain time on an Internet chat service, with DPR telling redandwhite, "I have something to discuss with you." Four days later, on June 5, 2013, DPR sent redandwhite a message stating, "hey, just wanted to find out where you are with the dummy ID idea." Redandwhite responded, "I have ran it by my worker and he is working on it."

43. Finally, the investigation has uncovered evidence implicating Ulbricht in running a Tor hidden service, and linking Ulbricht to certain programming code and a certain encryption key found on the Silk Road Web Server. Specifically:

a. Based on my training and experience, I know that the website "stackoverflow.com" ("Stack Overflow") is a website used by computer programmers to post questions about programming problems and to receive suggested solutions from other programmers. According to records obtained from Stack Overflow:

i. On March 5, 2012, a user established an account on Stack Overflow with the username "Ross Ulbricht." Ulbricht provided the Ulbricht Gmail Account as his e-mail address as part of his registration information.

ii. On March 16, 2012, at approximately 8:39 p.m. PDT, Ulbricht posted a message on the site, titled, "How can I connect to a Tor hidden service using curl in php?" Based on my training and experience, I know that "PHP" refers to a programming language used for web servers and "curl" refers to a set of programming commands that can be used in the language. In the contents of the message, Ulbricht quoted twelve lines of computer code involving "curl" commands that he stated he was using "to connect to a Tor hidden service using . . . php," but he reported the code was generating an error. Based on my training and experience, Ulbricht's posting reflects that he was writing a customized computer code designed for a web server operating a Tor hidden service, such as Silk Road.

iii. When a user posts a message on Stack Overflow, the user's username appears along with the post. However, less than one minute after posting the message described in the previous paragraph, Ulbricht changed his username at Stack Overflow from "Ross Ulbricht" to "frosty." Based on my training and experience, I know that criminals seeking to hide their identity online will often use

pseudonymous usernames to conceal their identity. Thus, given the timing, I believe that Ulbricht changed his username to "frosty" in order to conceal his association with the message he had posted one minute before, given that the posting was accessible to anyone on the Internet and implicated him in operating a Tor hidden service.

iv. Several weeks later, Ulbricht changed his registration e-mail on file with Stack Overflow as well, from the Ulbricht Gmail Account to "frosty@frosty.com." According to centralops.net, a publicly available e-mail address lookup service, "frosty@frosty.com" is not a valid e-mail address. Again, based on my training and experience, I know that criminals seeking to hide their identity online will often use fictitious e-mail addresses in subscribing to online accounts. Thus, I believe Ulbricht changed his e-mail address on file with Stack Overflow to a fictitious e-mail address in an attempt to eliminate any connection between his true e-mail address and his posting reflecting his operation of a hidden Tor service.

b. Based on forensic analysis of the Silk Road Web Server, I know that the computer code on the Silk Road Web Server includes a customized PHP script based on "curl" that is functionally very similar to the computer code described in Ulbricht's posting on Stack Overflow, and includes several lines of code that are identical to lines of code quoted in the posting. Based on my training and experience, it appears that the code on the Silk Road Web Server is a revised version of the code described in Ulbricht's posting (which Ulbricht stated in his posting he was seeking to fix given that it was generating an error).

c. Further, again, based on forensic analysis of the Silk Road Web Server, I know the following:

i. As of July 23, 2013, the Silk Road Web Server was configured to allow the administrator of the site, that is, DPR, to log in to the server without the need for a password, so long as the administrator logged in from a computer trusted by the server.

ii. Specifically, based on my training and experience, I know that this configuration involves the use of key-based secure shell ("SSH") logins. To set up this configuration, the administrator must generate a pair of encryption keys - a "public" key stored on the server, and a "private" key stored on the computer he logs into the server from. Once these keys are created, the server can recognize the

administrator's computer based on the link between the administrator's private key and the corresponding public key stored on the server.

iii. Based on my training and experience, I know that SSH encryption keys consist of long strings of text. Different SSH programs generate public keys in different ways, but they all generate public keys in a similar format, with the text string always ending with text in the format "[user]@[computer]". The computer in this substring represents the name of the computer that created the public key, and the user represents the username of the user who created it. For example, if someone creates an SSH key pair using a computer named "MyComputer," while logged into the computer as a user named "John," the public key generated as a result will end with the substring "John@MyComputer."

iv. I have examined the SSH public encryption key stored on the Silk Road Web Server that is used to authenticate administrative logins to the server. The key ends with the substring "frosty@frosty." Based on my training and experience, this means that the administrator of Silk Road has a computer named "frosty," on which he maintains a user account also named "frosty," which he uses to log in to the Silk Road Web Server. Based on my training and experience, I know that computer users often use the same username for different types of accounts. Thus, I believe, particularly given the other ties between "Ross Ulbricht" and "DPR" described above, that the Stack Overflow user "Ross Ulbricht," who changed his username to "frosty" and his e-mail address to "frosty@frosty.com," is the same person as the administrator of Silk Road, that is, DPR, who logs into the Silk Road Web Server from a computer named "frosty," on which he maintains a user account named "frosty."

44. I have obtained from the Texas Department of Motor Vehicles a copy of the driver's license of ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, bearing the same number as the driver's license that ULBRICHT showed to HSI agents during the July 26, 2013 interview described above. The photograph on the license depicts the same person appearing in the photographs of "Ross Ulbricht" on his profiles at Google+, the "Mises Institute," and LinkedIn described above.

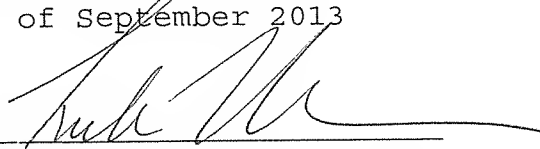
45. Accordingly, I believe that the owner and operator of Silk Road is ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant.

WHEREFORE, I respectfully request that an arrest warrant be issued for ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.



Christopher Tarbell
Special Agent
Federal Bureau of Investigation

Sworn to before me this
27th day of September 2013



HON. FRANK MAAS
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

EXHIBIT A



Silk Road

anonymous market

Shop by Category

messages 0 orders 0 account B0.0000

Search

Go

the Dread Pirate Roberts

Hi,

logout



From the forum

Buyer ratings discussion

Feedback system

changes

HOW TO: Run your own

relay and help the Tor

network

Ask a drug expert

physician about drugs

and health

Winning the war on

drugs

New display currencies

Try Taile for a more

secure OS

- Drugs 12,839
 - Cannabis 2,780
 - Dissociatives 136
 - Ecstasy 1,210
 - Intoxicants 75
 - Opioids 327
 - Other 91
- Precursors 78
- Prescription 4,382
- Psychedelics 1,673
- Stimulants 1,441
- Tobacco 217
- Apparel 702
- Art 14
- Books 1,285
- Collectibles 32
- Computer equipment 34
- Custom Orders 38
- Digital goods 801
- Drug paraphernalia 475
- Electronics 229
- Erotica 577
- Fireworks 34
- Food 12
- Forgeries 189
- Hardware 48
- Home & Garden 28
- Jewelry 100
- Lab Supplies 33
- Lottaries & games 163
- Medical 51
- Money 260
- Musical instruments 7
- Packaging 105
- Services 159
- Sporting goods 3
- Tickets 4
- Writing 8



1g High Quality Cocaine

B0.8956



HYDROPONIC BUD
224g(12lb) BULK BUY -

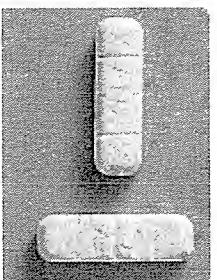
5 liters GBL 99.99% pure

1g 3-FA / crystalline powder



25HBOHle (hcl) 50mg

B0.2794



10 Xanax 2mg bars -USA
stock--

1.0 g Amphetamine Paste HQ
German Lab

25 LSD Blietters (United
Kingdom)

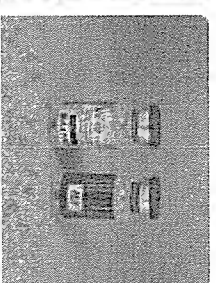
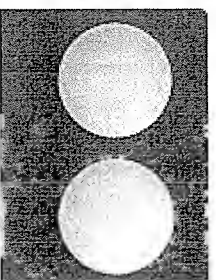


5G FLINSTONE
MEPHEDRONE, Yabba Dabba

10 x 10mg Oxycotin - OC
Formula Crush

10x 197 (Max Pro), 10ml,
197mg/ml

Custom Listing 50g HQ Pure
Cocaine



B1 = B1.0000

community forums wiki support

EXHIBIT B



Silk Road
anonymous market

Shop by Category

messages 0 orders 0 account \$0.0000

Search

Go

a few words from
the Dread Pirate Roberts

Hi,
logout



HIGH QUALITY #4 HEROIN ALL ROCK DIRECTLY FROM KEY

\$1.7198

[add to cart](#) [bookmark](#) [discuss 0](#) [report](#)

Item info:

seller: gotsitall 5.0
ships from: United States of America
ships to: United States of America
category: Heroin

postage options:

[COMBINE SHIPPING NC ?](#)

Description

-NEW BATCH 9/15/13 HIGH QUALITY # 4 HEROIN - THIS IS THE USUAL STUFF THAT I NORMALLY HAVE THAT IS WHY THE PRICE HAS GONE DOWN, LAST BATCH WAS THE KILLER FIRE H AND THAT HAS ENDED, I REPEAT THIS NEW BATCH IS THE NORMAL STUFF I USUALLY HAVE.

-THIS IS A MONDAY SHIPPING TUESDAY DELIVERY+ LISTING

-ALL ROCK

-NO POWDER

VACUUM SEALED

-STEALTH SHIPPING

-199\$/GRAM

-6 PM UTC CUTOFF TIME IF U ORDER AFTER YOUR ORDER WILL BE SHIPPED NEXT DAY.

---INSURANCE 12.00\$---

- BECAUSE OF CERTAIN PEOPLE GIVING ME PROBLEMS WITH SOME ORDERS I AM NOW OFFERING INSURANCE TO COVER YOUR PACKAGE IN THE EVENT THAT SOMETHING LISTED BELOW HAPPENS, INSURANCE WILL COVER EVERYTHING THAT HAPPENS AFTER I SHIP YOUR PACKAGE OUT, IF YOU DO NOT PURCHASE INSURANCE I WILL NOT RESHIP YOUR PACKAGE. INSURANCE WILL COVER EVERYTHING ONLY WHAT IS LISTED BELOW

-PACKAGE DID NOT RECEIVE ITS FIRST SCAN (LOST PACKAGE)

-PACKAGE WAS LOST IN THE MAIL (LOST AFTER INITIAL SCAN)

-PACKAGE WAS DAMAGED

-PACKAGE WAS MISSING CONTENT

-I TAKE A PICTURE OF EVERY PACKAGE MORE THEN 2 GRAMS SO JUST REMEMBER THAT BEFORE U CLAIM A MISSING CONTENT CLAIM I WILL MATCH WHAT U SAY TOWARD THE PICTURE I TAKE.

-PLEASE REMEMBER TO PURCHASE INSURANCE AS A PRECAUTION IF SOMETHING HAPPENED TO YOUR PACKAGE BECAUSE I WILL NOT RESHIP ANYTHING IF U DID NOT PURCHASE INSURANCE

-PGP KEY

---BEGIN PGP PUBLIC KEY BLOCK---

```
mQENBFGzOulBCADBPll1ayV5yACbXhbVZ1U+Cm+C7bF11dtGomvoW4b7DVdAtiv
8CqjXHD1P7VD+6p7GnVvrlK0seAq0eLhLoUJeJfF5tv7BVeusELr80u1DTwJR/9V
pJIZhm2P0EUNAMgmzzHkY78LKc/GXJ7XZn4cFB99UZ61wbCimEvTkdzj7pb/mCiq
f3ArkI/omS4B6nw13MjGw6YfRBn6H1dDK07AGWDFnS0oL8tuq806pg2h3Hhuwdg
Jy7Hxm80yNRgl4/yymZUt6iwpCAwFOiv584LGJiTIMj3z+uZoFPP4OL5USEPyU1
xxF/pbdcFI8xuRc6LhJAcl8Dg1f/10vXgp2XABEBAAG0IWdvdHNpdGFsbCA8Z290
```

c2IOYWxsQHRvcmlhaWwub3JnPokBPQQTaQoAJwUCUbM64glbLwUJB4YfgAULCQgH
AwUVCgkJCwUWAgMBAAlaAQIXgAAKCRDsUEPb2kt94ikBCACCEkyrTfzA3ErE/L3T
O/ND5Nw9w2bkuwJ66nzCkDPeUAKN3s6RXxa7cXejdR/hsDzd6iPpfEiVR/rh719
AMbTrFRaLXrluWppSt3zS/UKeuRilEPOFbA5N6mFSGIAaxzjFbhR1FKnAjWihsb
M6BW/cG5Rs6gd8fldzSHFOR/JrO8xyFpzNG0ZYzWkgdDtOmk+Va39C/PGSXG37a1
jNnqwyLjDUi9hsymcbfLtgO3FoXnZ8R7W2+jpGRdkyZWBfNt5OHnz546cnuj9yD3
ImZV7ZCwvvpkPRE/eMZEea6IOwSWm68R0/db4Dr9Se/vsuMcWVMMBF8c1JroU3Uq
6pzJuQENBF GzOulBCAC+ocVijQ0KVuh39dck5DCB5HFdkmnvUrLNczWcfSQLGQzt
3cVty6Cov8ITdvGH1TzZEZsZrvHLT/UBU2Ehwp+pQiPpcjredrpMeKessR1jfiMuA
tsASBlmjzYdPJ75vpgyPK3oW9zBHJ4aD/spvzBve69AWwxMeOgEATqe2OM2Klh2
Bapp95zFTv6ssDqdjnsCPwccYGdkkn4dJGOXqzY1kDwFktFzQ+Ct3QFWlS9NMMyCh
hzMiYEgPOWWhgKrtVs9y/xg8lj2tbiThbTQc6seISO1bdAmqedCaGaL/leqoOpP
FolxM5VQS68VWGEumlQqVLY30q17eE7K1BoU35tZABEBAAGJAkQEGAEKAA8FAIGz
OulCGy4FCQeGH4ABKQKQ7FBD29pLfeLAXSAEGQEKAAyFAIGzOulACgkQ6Hqp5mVK
VZVqtggAIVNcBLORDEgWM0bXOm+OnhfyIezBCulkegtCCfCa3IrfOfYcoGupz0
55vg/p6zNo0QZFUQWWalcs0oqy5/f+i2SWPeJaV7FgTWXpaCs5x77YSVeFhxWE/Q
nA8avJLUXUv001dc/54Bl8sn2mo1U6+TydXneXF1eX0mDuPctAdCf1Acg5hisfE
EdiXfJ5zbBAE2MNk1kxNhJK2Y4uUXVbhG+Odme3NJG/vuSwlpU0Rd9lfcVJpL+1
nBgJMJo5mniU54w7mqRDs1tQCGJViqCo5TLaf1SZ/NZ5mJ4Pybs3Dc3wNY4e44Yd
EmVhObk+0ETRUWnsgGfFckdZhVQeCx7B/0cnaTb+j3+RE2i3mu1INoozgKW/lSU
7DBQ8ISKNXUhuuETnYN6+jpXmxqv7zLdNQmUUTBO45M7aFR0NMGybMxf4OlHgUv
7buK1Go8JRnvqGEqhCKOVuP6KIKVY1yWVw7qyRJ4Y+TctRWclC5BNS69u5HsACS5
mOMXf1YomSdKhv4jX1UzhpP9lneqVgrllxwamjMVYxus1EsFI4GZ7dePy5rCg6q
lqarwMwp450IH2aE7M104CSgYjNuCKbt7YnbO3wEuGx1b5ZfJb/RDgX8lr4EdaO
K9XMqjcAFgd0OyFrT2Wq2hACi/Opikhvc5njinM81uwhoElr/Df7eEJOK
=Ryy3
-----END PGP PUBLIC KEY BLOCK-----

Reviews:

sort by:

weight

go

?

<div>themanwhocan</div> <div>orders spent vendors</div> <div>100+ <div>£100+</div> 10+</div>	<div>review for: HIGH QUALITY #4 HEROIN ALL ROCK DIRECTLY FROM KEY</div> <div>qty: 1 price: <div>£1+</div> 2d 14h old 5 of 5</div> <div>next day delivery made it the next day. was in transit shortly after i ordered. product is the same stuff as in picture and came in big chunks. Quality is superb, deffinitly worth the high price to get a more pure product which makes it more cost effective. Best stuff ive seen in awhile. its the real deal too non of that fent bullshit. just snorted a small bump and my pain is greatly reduced. thanks alot gotsitall ill be back!</div>
<div>Cobia</div> <div>orders spent vendors</div> <div>10+ <div>£100+</div> 10+</div>	<div>review for: HIGH QUALITY #4 HEROIN ALL ROCK DIRECTLY FROM KEY</div> <div>qty: 2 price: <div>£1+</div> 3d 18h old 5 of 5</div> <div>As others have made abundantly clear. gotsitall is an all around stand up guy. He has AMAZING products at more than reasonable prices and his customer support is some of the best I have ever encountered, I was missing some product, and he was just helpful and respectful the entire time, without the typical defensive anger most vendors would display any time there is any mention that product is missing. Through our discussions I was able to figure out what exactly went wrong (Sketchy asshole junky FOAF), and gotsitall was sympathetic and supportive thorough the whole process, even trying figure out how to help me to avoid withdrawal.</div> <div>TL;DR: Product 7/5 Awesome Dope (Best domestic stuff I've seen in a while) Customer Suppoprt/Attitude: 10/5 Just amazing. Shipping 6/5 Ordered Express Friday at 4pm. Order arrived Monday at 10am. Stealth 5/5 Nothing lacking here, sealed to be smell/detection proof, wrapped to look like standard mail.</div>
<div>alias hidden</div> <div>stats: (hidden)</div>	<div>review for: HIGH QUALITY #4 HEROIN ALL ROCK DIRECTLY FROM KEY</div> <div>1m 7d old 5 of 5</div> <div>horrible shipping time! but decent product and it was heavy. despite the b.s shitty shipping i will give 5/5 i feel it is a 5/5</div>
<div>alias hidden</div> <div>stats: (hidden)</div>	<div>review for: HIGH QUALITY #4 HEROIN ALL ROCK DIRECTLY FROM KEY</div> <div>1m 4d old 5 of 5</div> <div>leaving a 5/5 cuz GIA has never done me wrong so i dont want 1 hick up to reflect his legitimacy because he is the man but my last order was a bit weak for GIA's reputation, had to snort almost triple the amount of this new stuff to get where i was with the old. the product wasnt all rocks like stated(half powder half small rock)vendor didnt even address the fact that i was unhappy with my order but w.e this isnt walmart i guess. Either way GIA always come through and even when the product isnt his best its still probly top 2 of anything else on SR</div>
<div>alias hidden</div> <div>stats: (hidden)</div>	<div>review for: HIGH QUALITY #4 HEROIN ALL ROCK DIRECTLY FROM KEY</div> <div>1m 9d old 5 of 5</div> <div>Three cheers for GIA. Best vendor on SR! Got my product fast, at a killer price, with great customer service. A++++</div>
<div>A Friend</div> <div>orders spent vendors</div>	<div>review for: HIGH QUALITY #4 HEROIN ALL ROCK DIRECTLY FROM KEY</div> <div>qty: 2 price: <div>£1+</div> 3d 19h old 5 of 5</div> <div>Yeah!! ALL chunks off the brick as stated, definitely the GOODS, didn't start the day off</div>

10+ B100+ 10+	with it for the most accurate strength rating, but a very small shot cut through the fog admirably, dissolved completely in cool water, weight was on point or maybe 50mg. over, and delivery was speedy - what more could you ask, aside from quantity discounts? Thanks and praises be upon you!	
alias hidden stats: (hidden)	<i>review for: HIGH QUALITY #4 HEROIN ALL ROCK DIRECTLY FROM KEY</i> Great vendor, there was a mix up with the order but gotsitall took care of everything and fixed the situation. Will order again.	1m 4d old 5 of 5
AKMedSupply2013 orders spent vendors 10+ B100+ 10+	<i>review for: HIGH QUALITY #4 HEROIN ALL ROCK DIRECTLY FROM KEY</i> <i>qty: 1 price: B1+</i> 5/5 everytime!! Perfect stealth and perfect dope to match.Got product in less than 24 hours! Thanks again	15d 18h old unrated
radioheadfan5 orders spent vendors 100+ B100+ 10+	<i>review for: HIGH QUALITY #4 HEROIN ALL ROCK DIRECTLY FROM KEY</i> <i>qty: 2 price: B1+</i> Very fast shipping, great stealth, awesome product. You can't do better then GiA!	10d 17h old 5 of 5
alias hidden stats: (hidden)	<i>review for: HIGH QUALITY #4 HEROIN ALL ROCK DIRECTLY FROM KEY</i> on point. as always	1m 11d old 5 of 5